VASCO
THE AUTHENTICATION COMPANY

IDENTIKEY
server

Password Synchronization Manager

VACMAN Middleware & Identikey Server

User Manual

3.0

Disclaimer of Warranties and Limitations of Liabilities

The Product is provided on an 'as is' basis, without any other warranties, or conditions, express or implied, including but not limited to warranties of merchantable quality, merchantability of fitness for a particular purpose, or those arising by law, statute, usage of trade or course of dealing. The entire risk as to the results and performance of the product is assumed by you. Neither we nor our dealers or suppliers shall have any liability to you or any other person or entity for any indirect, incidental, special or consequential damages whatsoever, including but not limited to loss of revenue or profit, lost or damaged data of other commercial or economic loss, even if we have been advised of the possibility of such damages or they are foreseeable; or for claims by a third party. Our maximum aggregate liability to you, and that of our dealers and suppliers shall not exceed the amount paid by you for the Product. The limitations in this section shall apply whether or not the alleged breach or default is a breach of a fundamental condition or term, or a fundamental breach. Some states/countries do not allow the exclusion or limitation or liability for consequential or incidental damages so the above limitation may not apply to you.

Copyright

© 2008 VASCO Data Security. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of VASCO Data Security Inc.

Trademarks

DIGIPASS & VACMAN are registered trademarks of VASCO Data Security. All other trademarks or trade names are the property of their respective owners.

Table of Contents

1 Password Synchronization Manager 5
1.1 About this manual 6
1.1.1 How to Use this Manual 6
1.1.2 Document Conventions 6
1.1.3 Providing Feedback 7

2 Overview 8
2.1 Basic architecture 9
2.1.1 Synchronizing static passwords with VASCO Authentication Servers 10
2.1.2 Validating the availability of the VASCO Authentication Server 11
2.2 Basic requirements 12

3 Using PSM Configuration Application 13
3.1 Getting to Know PSM Configuration Application 14
3.1.1 Basic actions 14
3.2 General Settings Tab 15
3.3 VACMAN & Identikey Tab 18
3.3.1 VACMAN Middleware 3.0 with Active Directory 19
3.3.2 VACMAN Middleware 3.0 with database 20
3.3.3 Identikey Server 3.0 22
3.4 Auditing Tab 23
3.4.1 Using the Event Log 23
3.4.2 Using an additional debug log 24

4 Registry Reference Guide 25
4.1 General Settings 26
4.2 Password Filter Dynamic Loader settings 27
4.3 VACMAN/Identikey Filter settings 28

© 2008 VASCO Data Security. All rights reserved. Unauthorized duplication or distribution is prohibited.

Illustration Index

Figure 1: Password Synchronization Manager Architecture Overview 10

Figure 2: PSM Configuration Application Main Window -> Browse Servers....15

Figure 3: General Settings Tab -> Progress bar when refreshing server list....16

Figure 4: PSM Configuration Application Main Window -> General Settings 17

Figure 5: PSM Configuration -> VACMAN & Identikey Tab....18

Figure 6: PSM Configuration -> Connection Test....19

Figure 7: VACMAN & Identikey Tab -> VACMAN Middleware with Active Directory....20

Figure 8: VACMAN & Identikey Tab -> VACMAN Middleware using database 21

Figure 9: VACMAN & Identikey Tab -> Identikey Server 3.0 with database 22

Figure 10: PSM Configuration Application -> Auditing Tab 23

Index of Tables

Table 1: Domain Controller Icon States (Overview) 16

Table 2: PSM Status States (Overview)....16

© 2008 VASCO Data Security. All rights reserved. Unauthorized duplication or distribution is prohibited.

1 Password Synchronization Manager

Welcome to the Password Synchronization Manager (PSM) user manual. This document provides you the information you will need to use and configure PSM applications.

This manual provides information about how to:

- manage PSM using the PSM Configuration Application
- configure PSM to synchronize passwords with VASCO VACMAN Middleware 3.0
- configure PSM to synchronize passwords with VASCO Identikey Server 3.0
- troubleshoot and diagnose issues using the System Event Log and Debug Log

This manual does **not** provide:

- detailed instructions about preparing and installing the target systems (please refer to the respective product's Installation Guide)
- instructions about using PSM with other third-party applications

© 2008 VASCO Data Security. All rights reserved. Unauthorized duplication or distribution is prohibited.

1.1 About this manual

1.1.1 How to Use this Manual

You can use this manual in different ways, depending on your skill and knowledge level. You can read it from the beginning to the end (highly recommended for novice users), you can browse through the chapter abstracts and read specifically the chapters relevant to your needs, or you can search by key words in the index, if you need to find certain references quickly.

1.1.2 Document Conventions

The following typographic style conventions are used throughout this document.

Typography	Meaning
Boldface	Names of user interface widgets, e.g. the **OK** button
Blue	Values for options; placeholders for information or parameters that you provide, e.g. select Server name in the list box.
UPPERCASE	Keyboard keys, e.g. CTRL for the Control key
Monospace	Windows Registry Keys; commands you are supposed to type in or are displayed in a command prompt shell, including directories and filenames; API functions and source code examples
blue, underlined	Internet links

The following visual hint colour schemes are used throughout this document.

TIP
Tips contain supplementary information that is not essential to the completion of the task at hand, including explanations of possible results or alternative methods.

NOTE
Notes contain important supplementary information.

CAUTION
Cautions contain warnings about possible data loss, breaches of security, or other more serious problems.

© 2008 VASCO Data Security. All rights reserved. Unauthorized duplication or distribution is prohibited.

1.1.3 Providing Feedback

Every effort has been made to ensure the accuracy and usefulness of this manual. However, as the reader of this documentation, *you* are our most important critic and commentator. We appreciate your judgment and would like you to write us your opinions, suggestions, critics, questions, and ideas. Please send your commentary to: documentation@vasco.com.

To recognize the particular document you are referring to, please include the following information in your subject header: PSM-UM-3.0.0-03062008

Please note that product support is not offered through the above mail address.

© 2008 VASCO Data Security. All rights reserved. Unauthorized duplication or distribution is prohibited.

2 Overview

The purpose of the Password Synchronization Manger is to intercept user password changes in a Windows Domain environment and to synchronize them with other VASCO products.

The PSM for VM & IK 3.0 provides the following features:

Password synchronization of the Windows domain password to various target systems including:

- VASCO VACMAN Middleware 3.0
- VASCO Identikey Server 3.0

© 2008 VASCO Data Security. All rights reserved. Unauthorized duplication or distribution is prohibited.

2.1 Basic architecture

The PSM has a modular design to enhance its flexibility to accommodate the various requirements of customer software in the field.

It uses a standard Windows functionality called password filter, to intercept the user password to be changed. The password filter component of the PSM is subdivided into a general module and the specific modules for the target systems.

In this version the following target systems are supported:

- VASCO VACMAN Middleware 3.0
  - using Active Directory
  - using embedded or ODBC-compliant database
- VASCO Identikey Server 3.0
  - using embedded or ODBC-compliant database

The application-specific password filters use different methods to access their target systems.

The password filter for the VACMAN Middleware 3.0 and the Identikey Server 3.0 is implemented in one module and uses the VASCO AAL3 libraries and its SEAL API to access the authentication server and the Digipass User store.

Due to the architecture since Windows 2000, every domain controller within the domain/directory is able to serve password change requests (in Windows NT 4.0 and earlier, only the primary domain controller was able to serve them), the PSM *must* be installed on every domain controller in order to not loose any password changes.

© 2008 VASCO Data Security. All rights reserved. Unauthorized duplication or distribution is prohibited.

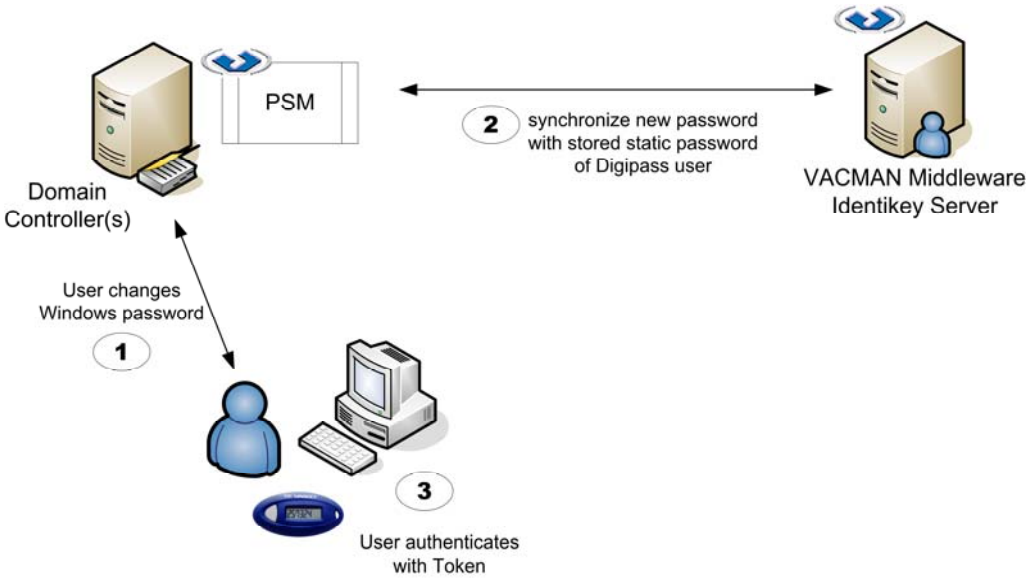

Figure 1: Password Synchronization Manager Architecture Overview

NOTE
In the process of installation of the PSM all the domain controllers have to be restarted.

CAUTION
Problems or misconfiguration of the PSM could lead to problems in the domain. Please make sure that the configuration is validated and all settings are working.

2.1.1 Synchronizing static passwords with VASCO Authentication Servers

A Digipass User account has a Stored Static Password field. When Back-End Authentication is used, this field can be used to store the static password required for Back-End Authentication. This means that the user does not need to type in the static password at each login. He only needs to enter the OTP. VACMAN Middleware or the Identikey Server can retrieve the Stored Static Password from the Digipass User account and use it for Back-End Authentication.

When a user uses a token to replace his Windows static password, and this static password changes, he needs to re-synchronize his Digipass user account with the new password. If no password synchronization is used this has to be done manually by the user.

The PSM can be used to perform this task automatically so that there is no more manual interaction necessary.

When the Windows user password is changed, the Static Password store in the Digipass user account will be updated with the new password.

© 2008 VASCO Data Security. All rights reserved. Unauthorized duplication or distribution is prohibited.

2.1.2 Validating the availability of the VASCO Authentication Server

A successful password synchronization process depends on the availability of all involved target systems. The PSM is designed to check if the target system is available before the actual password change takes place.

If the target system can not be reached the PSM software will deny the password change request and Windows will be notified that there was a problem. Windows will therefore deny the password change request also to the other password filter modules and eventually to the user. The current password will not be changed.

If the check is not performed the function of the password synchronization is not secured. If a password change is not performed on all configured target systems the password will be out of sync and the user will not be able to log on to these systems.

CAUTION
The system availability check can be disabled but it is not recommended as it will lead to problems with the synchrony of passwords between the Windows domain and the applications. In case of problems please check the Windows Event Log and the communication between the domain controllers, the PSM and the target systems.

© 2008 VASCO Data Security. All rights reserved. Unauthorized duplication or distribution is prohibited.

2.2 Basic requirements

For the installation and configuration of the PSM you need the following information about your VACMAN Middleware 3.0 or Identikey Server 3.0 environment:

- IP addresses (or names) of the authentication server and its backup servers
- Port number for the SEAL communication
- Type of DIGIPASS datastore (Active Directory or database)
- XML Configuration

© 2008 VASCO Data Security. All rights reserved. Unauthorized duplication or distribution is prohibited.

3 Using PSM Configuration Application

PSM Configuration Application is an administration tool allowing you to manage the settings on the PSM on your domain controllers. This chapter gives an overview of the tool and how to use it.

NOTE
You have to have domain administrative rights to perform the necessary configuration tasks.

It covers the following topics:

- Getting to Know PSM Configuration Application

© 2008 VASCO Data Security. All rights reserved. Unauthorized duplication or distribution is prohibited.

3.1 Getting to Know PSM Configuration Application

➢ To start PSM Configuration Application

- Select **Start > Programs > VASCO > Password Synchronization Manager > PSM Configuration**.

3.1.1 Basic actions

➢ To confirm and activate the configuration settings

- The configuration settings will be set when the application is closed by selecting **OK** or **Apply**.

The configuration settings are valid for all domain controllers where the PSM is installed and. With applying the settings the PSM will be temporarily set into maintenance mode and the changes will be written back to the local registry of each domain controller. The PSM will be activated immediately after that and the settings will be reloaded by each PSM module.

© 2008 VASCO Data Security. All rights reserved. Unauthorized duplication or distribution is prohibited.

3.2 General Settings Tab

Upon startup, the current domain will be browsed and all domain controllers are displayed in a list view. By default, all domain controllers will be checked. As this can take some time in bigger environments, a progress bar will be displayed. The progress bar will be shown only if a browse operation is active.

The settings of the first domain controller will be retrieved and imported into the local registry. Please be aware that the current local settings will be overwritten.

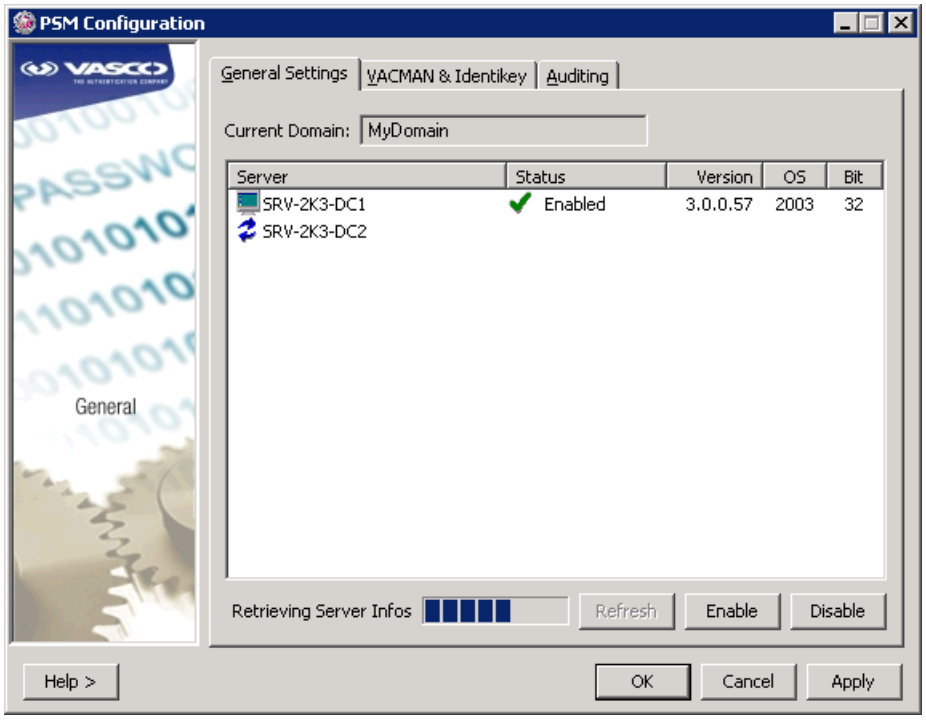

Figure 2: PSM Configuration Application Main Window -> Browse Servers

If the PSM is installed on the domain controller its status will be displayed (see table below). Additional information like the PSM version number and the OS version of the domain controller will be displayed.

Domain Controller List (Icon)	Meaning
	Status: OK. Domain Controller could be contacted and configuration data was retrieved.
	Status: In progress. Configuration data is being retrieved.

© 2008 VASCO Data Security. All rights reserved. Unauthorized duplication or distribution is prohibited.

Table 1: Domain Controller Icon States (Overview)

PSM Status	Meaning
Enabled	Status: OK. PSM is installed and enabled.
Not Installed	Status: Error. PSM is not installed on this domain controller or configuration data could not be retrieved.
Maintenance	Status: Warning. PSM is in maintenance mode on this particular domain controller. Password changes handled by this domain controller will fail.
Disabled	Status: Error. PSM is installed, but disabled. Password changes will not be synchronized.

Table 2: PSM Status States (Overview)

➢ To refresh the list of domain controllers

- Select **Refresh** to initiate the browse operation. A progress bar will be displayed.

Figure 3: General Settings Tab -> Progress bar when refreshing server list

➢ To enable PSM

- Select **Enable** to enable the PSM for the current domain.

➢ To disable PSM

- Select **Disable** to disable the PSM for the current domain.

NOTE
Enabling and disabling the PSM can only be performed for all domain controllers.

© 2008 VASCO Data Security. All rights reserved. Unauthorized duplication or distribution is prohibited.

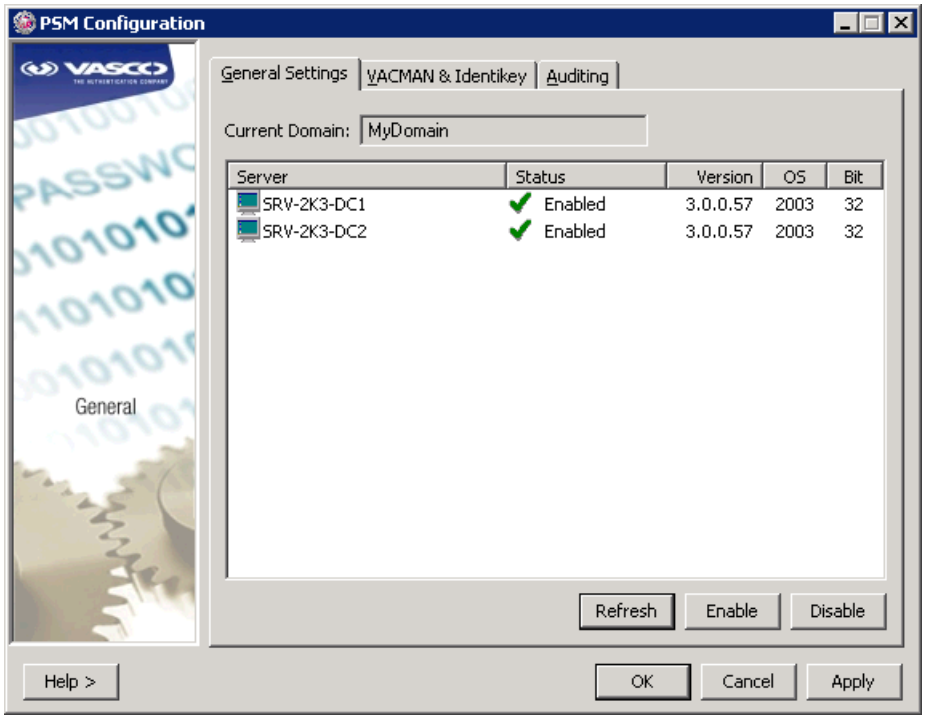

Figure 4: PSM Configuration Application Main Window -> General Settings

© 2008 VASCO Data Security. All rights reserved. Unauthorized duplication or distribution is prohibited.

3.3 VACMAN & Identikey Tab

The basic parameters of the connection settings to the VASCO authentication servers can be configured on this tab page.

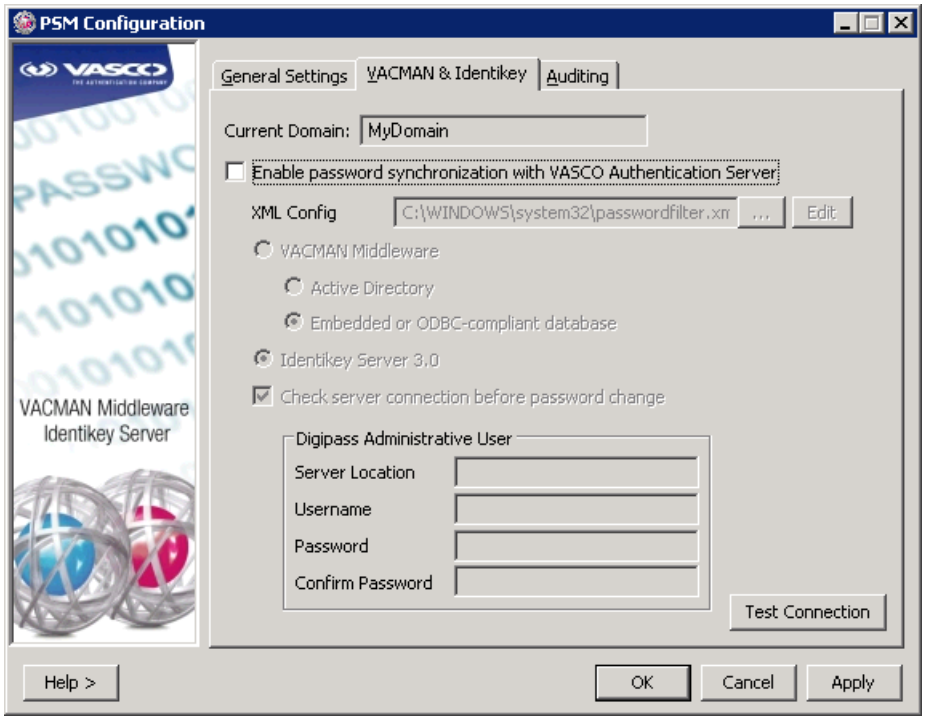

Figure 5: PSM Configuration -> VACMAN & Identikey Tab

➢ To enable the VACMAN & Identikey module of PSM

- Select the **Enable password synchronization with VASCO Authentication Server** to activate the module

➢ To configure the connection settings through external XML file

1. For the configuration of the connection to the primary VASCO Authentication Server and the AAL3 libraries a XML configuration file is necessary. The path and filename can be configured in the **XML Config** field.
2. Select **...** to browse for the configuration file.
3. Select **Edit** to open the configuration file.

© 2008 VASCO Data Security. All rights reserved. Unauthorized duplication or distribution is prohibited.

NOTE
Edit opens the selected file using the default action that is configured in Windows for the particular file type. Please make sure that you have registered a default application to edit XML files.

CAUTION
If you edit the XML configuration file, you are only editing the local file on the server where you opened the management tool. If you make changes to the XML configuration file you have to copy the new file to the same location on every domain controller.

To set the correct connections parameters for the different VASCO Authentication Servers the administrator has to set the corresponding options. Please refer to the user manuals of the respective products for more information how to prepare the XML configuration file.

➢ To enable the target system availability check while the password change process

- Select **Check server connection before password change**

➢ To validate the current connections settings manually

- Select **Test Connection** and wait for the response.

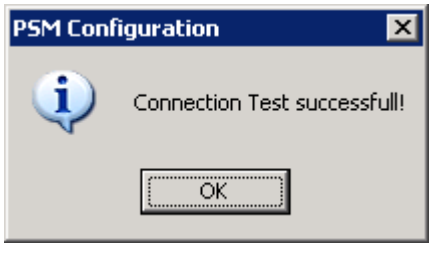

Figure 6: PSM Configuration -> Connection Test

3.3.1 VACMAN Middleware 3.0 with Active Directory

If the used VACMAN Middleware 3.0 Authentication Server is using Active Directory as its data store you have to configure the following settings.

© 2008 VASCO Data Security. All rights reserved. Unauthorized duplication or distribution is prohibited.

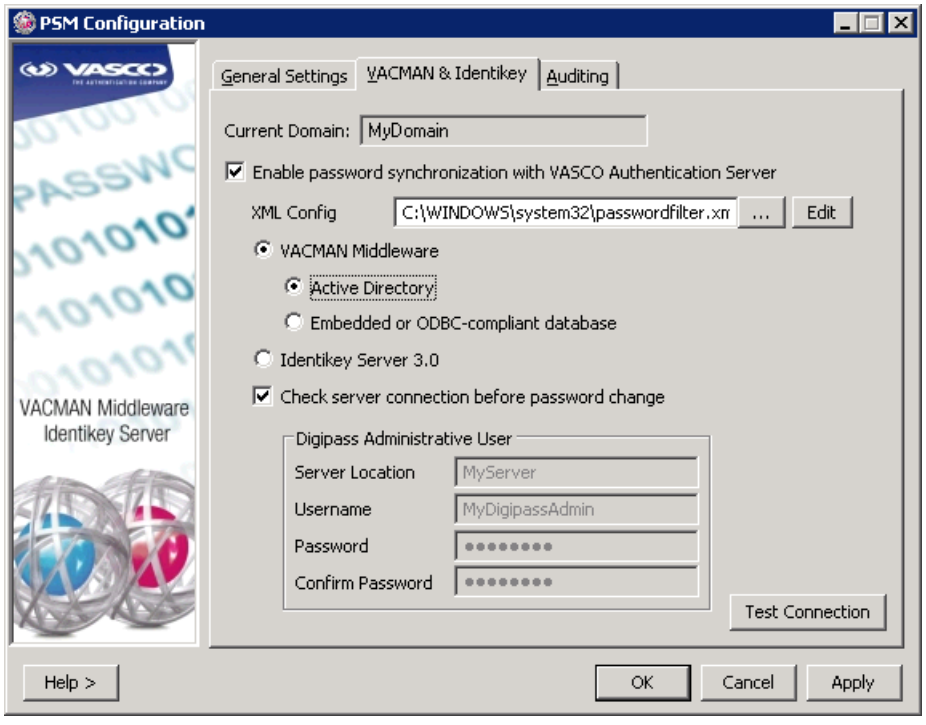

Figure 7: VACMAN & Identikey Tab -> VACMAN Middleware with Active Directory

➢ To enable VACMAN Middleware 3.0 with Active Directory

1. Select **VACMAN Middleware**
2. Select **Active Directory**
3. Select **Apply** to confirm and save the settings
4. Select **Test Connection** to validate the configuration

NOTE
If you have installed the PSM Configuration Application on a client machine, you cannot use **Test Connection** to validate the Active Directory connection. The test will fail. This test will work only on a domain controller.

3.3.2 VACMAN Middleware 3.0 with database

If the used VACMAN Middleware 3.0 Authentication Server is using an embedded or ODBC-compliant database as its data store you have to configure the following settings.

© 2008 VASCO Data Security. All rights reserved. Unauthorized duplication or distribution is prohibited.

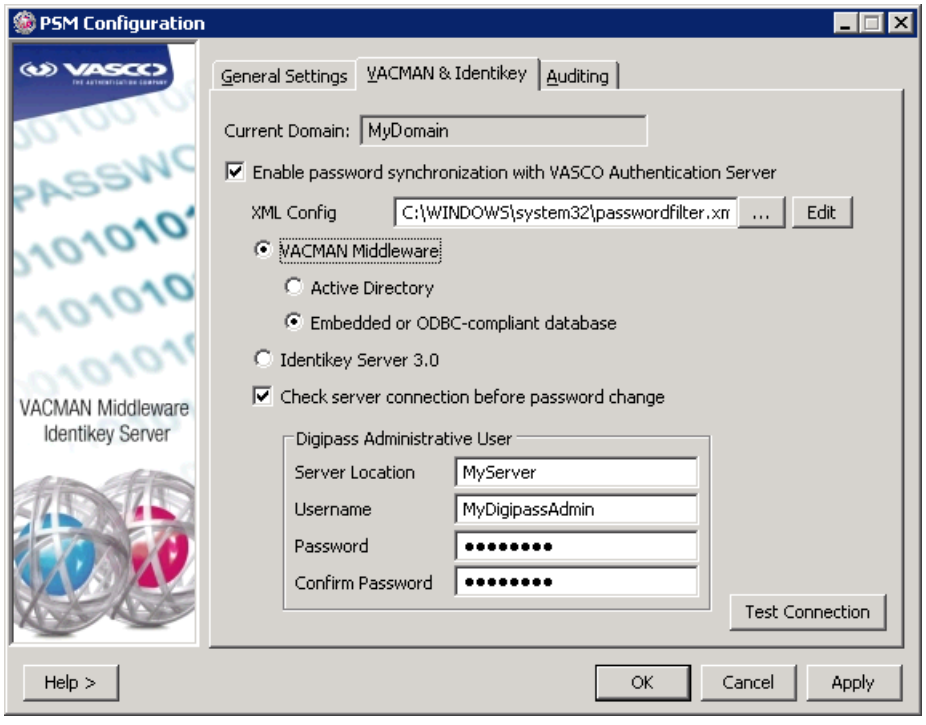

Figure 8: VACMAN & Identikey Tab -> VACMAN Middleware using database

➢ To enable VACMAN Middleware 3.0 with database

1. Select **VACMAN Middleware**
2. Select **Embedded or ODBC-compliant database**

➢ To configure the Digipass Administrative User

1. Enter the IP address or the name of the Authentication Server in the **Server Location** field
2. Enter the username of the Digipass Administrative User in the **Username** field
3. Enter the password of the Digipass Administrative User in the **Password** field
4. Re-enter the password of the Digipass Administrative User in the **Confirm Password** field
5. Select **Apply** to confirm and save the settings
6. Select **Test Connection** to validate the connection parameters

© 2008 VASCO Data Security. All rights reserved. Unauthorized duplication or distribution is prohibited.

3.3.3 Identikey Server 3.0

If the Identikey Server 3.0 is using an embedded or ODBC-compliant database as its data store you have to configure the following settings.

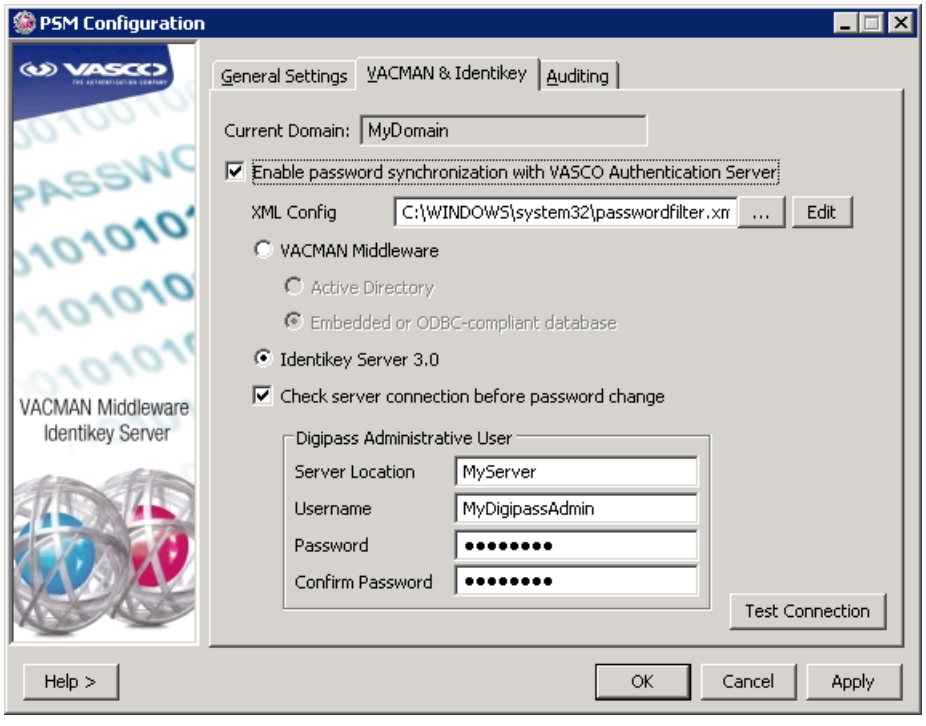

Figure 9: VACMAN & Identikey Tab -> Identikey Server 3.0 with database

➢ To enable Identikey Server 3.0

1. Select **Identikey Server 3.0**

➢ To configure the Digipass Administrative User

1. Enter the IP address or the name of the Authentication Server in the **Server Location** field
2. Enter the username of the Digipass Administrative User in the **Username** field
3. Enter the password of the Digipass Administrative User in the **Password** field
4. Re-enter the password of the Digipass Administrative User in the **Confirm Password** field
5. Select **Apply** to confirm and save the settings
6. Select **Test Connection** to validate the connection settings

© 2008 VASCO Data Security. All rights reserved. Unauthorized duplication or distribution is prohibited.

3.4 Auditing Tab

The auditing settings can be set in this tab page. It is highly recommended to enable these settings as they may help in case of troubleshooting.

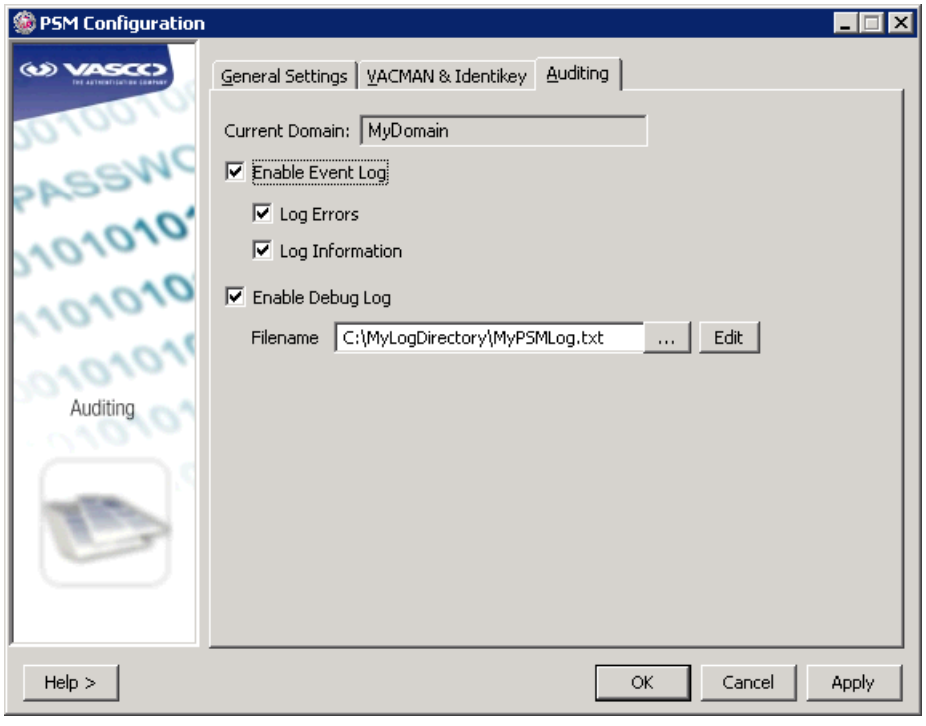

Figure 10: PSM Configuration Application -> Auditing Tab

3.4.1 Using the Event Log

General events and configuration errors of the PSM can be easily traced using the entries in the Windows Event Log. If you have a multi-domain controller environment, and as the actual password change can occur everywhere, the administrator has to check every Event Log, if an error occurs.

➢ To enable the Event Log

1. Select **Enable Event Log**
2. Select **Log Errors** to enable the logging of errors
3. Select **Log Information** to enable the logging of general events

© 2008 VASCO Data Security. All rights reserved. Unauthorized duplication or distribution is prohibited.

3.4.2 Using an additional debug log

For more detailed information and for support reasons you can enable also a debug log, which will be written to a text file and has to be specified by path and filename.

➢ To enable the Debug Log

1. Select **Enable Debug Log**
2. Select **...** to browse for a debug log file
3. Select **Edit** to open the debug log file

NOTE
Edit opens the selected file using the default action that is configured in Windows for the particular file type. Please make sure that you have registered a default application to edit text files.

CAUTION
If you setup a debug log file, the file will be created locally on every server with the path and filename you have configured in the settings. Please make sure that the path and filename is valid for all domain controllers.

© 2008 VASCO Data Security. All rights reserved. Unauthorized duplication or distribution is prohibited.

4 Registry Reference Guide

The PSM can be configured through additional registry parameters if needed. However the values should only be changed if you know what you are doing or being advised by VASCO support.

CAUTION
Be careful with changes in the registry. It is recommended to use the PSM Configuration Application to change the settings.

Any change has immediate effect and no reboot is necessary. However, it is necessary to reload the password filters. You can do this manually by setting the PSM to the Maintenance Mode and then enable it again.

Please note that if you make manual changes to the local registry on a domain controller, these changes will not be synchronized with the other domain controllers where the PSM is installed. However, if you start the PSM Configuration Application, the local settings will be overwritten with the settings of the first server in the list. The manual configuration of the settings is useful, if the configuration settings on the domain controllers can not be the same.

The following registry settings are used to store the configuration of the PSM.

© 2008 VASCO Data Security. All rights reserved. Unauthorized duplication or distribution is prohibited.

4.1 General Settings

PSM can log its internal events for troubleshooting into the System Event Log and/or into a text file.

[HKEY_LOCAL_MACHINE\SOFTWARE\VASCO Data Security\PasswordSyncManager]

Name	Type	Description
LogSettings	REG_DWORD	This value sets the logging options (bitmapped). Bit 0: disabled Bit 1: enable log to EventLog Bit 2: log errors to EventLog Bit 3: log info to EventLog Mask with 0x80000000 to enable debug log to file. The default value is 7.
DebugLogPath	REG_SZ	Path and filename of the Debug Log file This value is not set by default.

© 2008 VASCO Data Security. All rights reserved. Unauthorized duplication or distribution is prohibited.

4.2 Password Filter Dynamic Loader settings

The settings for the Password Filter Dynamic Loader consist of the list of the password filters DLLs to be loaded and the status settings for the PWFDL.

[HKLM\SOFTWARE\VASCO Data Security\PasswordSyncManager\DynamicLoader]

Name	Type	Description
Filters	REG_MULTI_SZ	Name of the password filter DLLs (with the .DLL extension). The path information is optional if not installed in PATH. The value is set by the installer.
MaintenanceTimeout	REG_DWORD	Timeout in the Maintenance Mode of the PWFDL before a password change is aborted. The value is set in milliseconds. The default value is 20000.
Status	REG_DWORD	This value represents the actual status of the PWFDL. It can be set from an external source to change the internal state of the PWFDL. 1: Enabled 2: Disabled 3: Maintenance mode The default value is 1. The Maintenance Mode is used to unload the password filter(s) in case of an update of the binary modules or configuration changes. While in maintenance mode the password change requests are blocked. See also value 'MaintenanceTimeout'.

© 2008 VASCO Data Security. All rights reserved. Unauthorized duplication or distribution is prohibited.

4.3 VACMAN/Identikey Filter settings

The VMPWFilt module is the password filter library to synchronize the Windows passwords with the VASCO Authentication servers.

[HKLM\SOFTWARE\VASCO Data Security\PasswordSyncManager\Vacman]

Name	Type	Description
XMLPath	REG_SZ	This value contains the path and filename of the configuration XML file for the AAL3 library. The PSM installer installs a default configuration file. The default value is '<InstallDir>\passwordfilter.xml'. This value is set by the installer.
LoginName	REG_SZ	Administrative Login Name This value is not set by default.
EncryptedPassword	REG_BINARY	Encrypted Administrative password (AES256) This value is not set by default.
Settings	REG_DWORD	This value sets the basic VMPWFilt settings. This value is bitmapped. Bit 0: Enable VMPWFilt filtering Bit 1: VACMAN Middleware support 0 = ODBC Database 1 = Active Directory Bit 2: Enable Identikey Server support 1 = ODBC Database Bit 3: Enable target system availability check Remark: The Active Directory support for Identikey Server is not implemented. The default value is 12.

© 2008 VASCO Data Security. All rights reserved. Unauthorized duplication or distribution is prohibited.